ARGUMENT

I. J-STD-025 Satisfies the Capability Requirements of Section 103(a) of CALEA and Is Not "Deficient"

This rulemaking proceeding involves a single narrow set of issues – i.e., whether, for the reasons advanced by DOJ, FBI and CDT, J-STD-025 is "deficient" for failure to satisfy the assistance capability requirements of Section 103(a) of CALEA. It is undisputed that J-STD-025 is a properly-adopted interim industry standard[44] that – if not "deficient" – satisfies the requirements of the "safe harbor" of Section 107(a)(2) of CALEA.[45] For the reasons set out in detail below, the Commission should conclude that J-STD-025 is in fact not "deficient."

---

[44] Thirty-six months after publication of J-STD-025 (i.e., in December 2000), TIA intends to submit J-STD-025 to the American National Standards Institute for final approval as an American National Standard. See J-STD-025, "Interim Standards" notice.

[45] Section 107(a)(2) provides:

> COMPLIANCE UNDER ACCEPTED STANDARDS. – A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under [Section 107(b)], to meet the requirements of section 103.

47 U.S.C. § 1006(a)(2) (emphasis added).

A. The Role of the Commission Under CALEA Is Limited to Determining Whether J-STD-025 Is "Deficient"

Section 103(a) of CALEA specifies four types of assistance capability requirements that telecommunications carriers must satisfy:

- expeditious delivery of the content of "all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission";[46]
- expeditious delivery of "call-identifying information that is reasonably available to the carrier";[47]
- delivery of communications and call-identifying information to law enforcement at a remote location;[48] and
- facilitating unobtrusive interceptions that protect (1) the "privacy and security" of communications and (2) government information regarding interceptions.[49]

As discussed in detail below, the DOJ/FBI Petition alleges that J-STD-025 fails to provides one capability covered by the first requirement, and fails to provide several capabilities covered by the second requirement. There are no allegations of deficiency with respect to the third requirement. The CDT Petition alleges that two provisions J-STD-025 are inconsistent with the component of the fourth requirement relating to privacy of communications. These are the only matters at issue in this rulemaking proceeding.

---

[46] 47 U.S.C. § 1002(a)(1).

[47] 47 U.S.C. § 1002(a)(2).

[48] 47 U.S.C. § 1002(a)(3).

[49] 47 U.S.C. § 1002(a)(4).

It is critical that the Commission recognize that the failure to provide the capabilities mandated by Section 103(a) is the **sole** statutory basis on which it could conclude that J-STD-025 is "deficient." Indeed, the legislative history of CALEA explicitly states that the requirements of Section 103(a) are intended as "both a floor and ceiling" for CALEA obligations.[50] These considerations are particularly important because the DOJ/FBI Petition bases many of its challenges to J-STD-025 on arguments that have little or nothing to do with the capability requirements of Section 103(a).

J-STD-025 represents an effort by the telecommunications industry fully to satisfy each of the requirements of Section 103(a). As contemplated by Section 107(a)(1) of CALEA,[51] telecommunications carriers and equipment manufacturers have worked with the law enforcement community for more than three years to develop an understanding of law enforcement requirements and to seek an interpretation of the Section 103(a) capability requirements that provides maximum assistance to law enforcement within the boundaries established by CALEA.[52] TIA is confident that the Commission will upon review conclude that J-STD-025 does in fact satisfy each of the requirements of Section 103(a).

---

[50] CALEA House Report at 22.

[51] 47 U.S.C. § 1006(a)(1) ("law enforcement agencies . . . shall consult with appropriate associations and standard-setting organizations of the telecommunications industry, with representatives of users of telecommunications equipment, facilities, and services").

[52] The FBI itself has recently acknowledged "the good faith efforts of [industry] solution providers and carriers in developing a CALEA solution . . . ." 1998 Implementation Report at 15 (Jan. 26, 1998).

In Section 107(a)(2) of CALEA,[53] Congress made it clear that the telecommunications industry has the primary role in CALEA standards-setting. The Congressional delegation to industry of primary responsibility for CALEA standards-setting is highly appropriate. It is established law that Congress has authority to delegate to an industry association the authority to establish legally binding standards,[54] and telecommunications standards bodies have extensive experience regarding the complex issues associated with design and operation of telecommunications networks. Furthermore, as noted in the TIA Petition, the frequent use of multiple manufacturers' equipment in a single carrier's network requires standards-based, compatible solutions to ensure that such equipment is fully interoperable.[55] Subtle design differences could cause system incompatibility, network unreliability and even failure.

The Commission is permitted to modify industry-established CALEA standards, but only if they are "deficient." Specifically, Section 107(b) of CALEA provides:

> if a Government agency or any other person believes that [industry] requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards . . . .[56]

---

[53] 47 U.S.C. § 1006(a)(2).

[54] See St. Louis, Iron Mountain & So. R.R. v. Taylor, 210 U.S. 281, 285-87 (1908) (upholding delegation to American Railway Association of authority to set standard height for freight cars); Crain v. First National Bank of Oregon, 324 F.2d 532, 537 (9th Cir. 1963) ("While Congress cannot delegate to private corporations or anyone else the power to enact laws, it may employ them in an administrative capacity to carry them into effect.").

[55] See TIA Petition at 6-7.

[56] 47 U.S.C. § 1006(b).

The role of law enforcement in CALEA standards-setting is limited to the right to consult with the telecommunications industry[57] and the right (shared with "any other person") to petition the Commission for a determination that an industry standard is "deficient."[58]

Section 107(b) of CALEA provides that in considering whether an industry standard is "deficient," the Commission may only consider alternative standards that

> (1) meet the assistance capability requirements of section 103 by cost effective methods;
>
> (2) protect the privacy and security of communications not authorized to be intercepted;
>
> (3) minimize the cost of such compliance on residential ratepayers; [and]
>
> (4) serve the policy of the United States to encourage the provision of new technologies and services to the public."[59]

Congress was clear that the Commission, in reviewing such challenges to an industry standard, must comply with these statutory factors.[60]

---

[57] 47 U.S.C. § 1006(a)(1).

[58] 47 U.S.C. § 1006(b).

[59] 47 U.S.C. § 1006(b)(1)-(4). In addition, Section 107(b) requires the Commission to "provide a reasonable time and conditions for compliance with and transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period." 47 U.S.C. § 1006(b)(5). This factor is addressed in the TIA Extension Comments and the TIA Extension Reply Comments.

[60] See, e.g., CALEA House Report at 27 ("In taking any action under this section, the FCC is directed to protect privacy and security of communications that are not the targets of court-ordered electronic surveillance and to serve the policy of the United States to encourage the provision of new technologies and services to the public.").

In sum, the Commission should confine its inquiry in this proceeding to whether J-STD-025 is "deficient" for failure to satisfy the capability requirements of Section 103(a), and should not entertain the alternative arguments not based in the text of CALEA that DOJ and FBI advance. Furthermore, the Commission should take care that its inquiry is informed by consideration of the four key statutory factors set out in Section 107(b) of CALEA.

B. The DOJ/FBI Petition and CDT Petition Do Not Assert Any Basis on Which the Commission Could Properly Conclude that J-STD-025 Is "Deficient"

The Commission should deny the DOJ/FBI Petition and the CDT Petition, because the petitions do not provide any proper basis for a conclusion that J-STD-025 is "deficient." For the reasons set out in detail in Sections II-VI below, J-STD-025 fulfills each of the assistance capability requirements of Section 103(a), and the various arguments to the contrary of the DOJ, FBI and CDT fail for a variety of reasons that are also addressed in detail in those sections.

By contrast, the proposed modifications to J-STD-025 – particularly the punch list items requested by DOJ and FBI – would violate Section 103(a). As the telecommunications industry, privacy groups, and even members of Congress have stated, each of the DOJ/FBI punch list requirements exceeds the scope of CALEA.[61] Many of the

---

[61] Several members of Congress have since agreed with the assessment of industry and the privacy groups. See, e.g., 143 Cong. Rec. H10939 (daily ed. Nov. 13, 1997) (statement of Rep. Barr) ("I have also concluded that law enforcement has been using CALEA to overreach, and that the FBI is looking to use CALEA for the perfect solution to their wiretapping wishes. Indeed, many of the so-called 'punch-list' items clearly are beyond the scope of the Act."); Letter from Senator Patrick Leahy to Attorney

(Continued ...)

punch list items request capabilities that are clearly not required to be provided under Section 103(a). Furthermore, some of the punch list items (e.g., interception of conversations of parties on hold) threaten individual privacy, permitting law enforcement to intercept communications that are not authorized to be intercepted under Title III.

With respect to many of the requested capabilities requested in the DOJ/FBI Petition, DOJ and FBI do not articulate in sufficient detail the specific nature of the capabilities sought – making it extremely difficult for the Commission and the telecommunications industry to assess the requested capabilities. In fact, the unwillingness of DOJ and FBI to provide such detail has been a persistent problem during the three-year negotiations over CALEA implementation. In the context of the present rulemaking, the absence of detail means that the Commission in many areas lacks any actual factual basis for a conclusion that J-STD-025 is "deficient."

Implementation of the punch list capabilities would also impose tremendous costs that would violate the requirements of Section 107(b) that interception capability be implemented by the most cost-effective methods; that the cost on residential ratepayers be minimized; and that the provision of new technologies and services be encouraged. There is simply no legal basis for the Commission to impose on carriers the unnecessary costs that would be associated with capabilities not required by CALEA.

General Janet Reno and Director Louis Freeh (Feb. 4, 1998) ("I understand that a proposed industry standard, SP-3580A, was circulated for adoption by carriers last year and that this standard, if adopted, would have solved the majority of the 'digital telephony' problems identified by the FBI during congressional deliberation of this law. Nevertheless, the FBI criticized this standard for failing to provide a limited number of eleven functions (or 'punch list capabilities'). Certain of these punch list items appear far beyond the scope and intent of CALEA . . .").

Imposition of these costs is also not necessary to protect the effectiveness of law enforcement, as the DOJ/FBI Petition repeatedly suggests. Rather, since J-STD-025 already fully satisfies the legitimate interception requirements of law enforcement, the real issue is cost versus convenience to law enforcement (since many of the punch list tasks would make law enforcement's job easier). While easing burdens on law enforcement is a worthwhile goal, it is not a proper basis for concluding that J-STD-025 is "deficient." Furthermore, there is no reason for the Commission to conclude that the telecommunications industry has declined to implement the punch list in order to avoid costs that CALEA legitimately imposes. To the contrary, the industry has significant financial incentives to adopt standards that are fully compliant with CALEA, in order to avoid major redesign costs if the standard is found to be "deficient."

In sum, for the reasons set out in these comments, the DOJ/FBI Petition does not provide any basis for a conclusion that J-STD-025 fails to comply with the assistance capability requirements of Section 103(a) of CALEA. Likewise, the privacy concerns raised in the CDT Petition do not justify CDT's requested changes to J-STD-025. Therefore, the Commission should conclude that J-STD-025 is not "deficient."

C. The DOJ/FBI Argument Regarding Historical Availability of Interception Capabilities Is Not Supported by CALEA

Perhaps the most significant weakness of the DOJ/FBI Petition is its contention that CALEA "mak[es] available the same kinds of information about a subscriber's services and their use that has always been available to law enforcement

officers."[62] This argument that is repeated throughout the petition is entirely unsupported by CALEA.

Historically, DOJ and FBI conducted interceptions by attaching a recording device, a "pen register" (which records numbers dialed), or a "trap and trace" device (which records the source of incoming calls) to the copper wire "local loop" between the customer and the telephone company switch. DOJ and FBI contend that the information that has "always been available" on such local loop interceptions should also be available on interceptions pursuant to CALEA.

This "always been available" argument has no source in the text of CALEA. Furthermore, even if the argument did have a statutory basis, DOJ and FBI fail to provide any concrete information on the types of information that has "always been available" on local loop intercepts. Accordingly, in order to adopt this argument of DOJ and FBI, the Commission would need to rely on a legal doctrine that is contrary to CALEA and to speculate regarding the factual basis for applying that doctrine.

The premise for the DOJ/FBI "always been available" argument is that the Congressional purpose for passing CALEA was "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies . . . ."[63] Congress did not choose to effectuate this purpose,

---

[62] DOJ/FBI Petition at 19 (emphasis added); see also id. at 26 ("In many respects, the provisions of the proposed rule concern communications and call-identifying information that law enforcement historically has received.").

[63] CALEA House Report at 9; see DOJ/FBI Petition at 19 ("CALEA was . . . designed to enable law enforcement agencies to keep pace with rapidly changing telecommunications technologies by preserving law enforcement officers' access to all communications authorized to be intercepted . . . .").

however, by providing that law enforcement would have access to the same intercept information that it has received in the past. Such an approach would have been unworkable for at least two significant reasons.

First, changing technologies mean that information relating to intercepts also changes. Frequently, such changes increase the amount (and the accessibility) of information available to law enforcement. **Second**, as an evidentiary matter, it would be extremely difficult for industry, law enforcement and the Commission to determine precisely what intercept capabilities have historically been available, and to decide what the equivalent capabilities are with respect to each new technology. If the DOJ/FBI "always been available" approach were substituted for the market-based "reasonable availability" approach that is explicit in the text of CALEA, wiretap capabilities for each new technology would need to be analyzed in terms of law enforcement capabilities at an arbitrary point in the past, rather than permitting reliance on industry standards reflecting present technologies, as Congress clearly contemplated in adopting CALEA. The result of the DOJ/FBI approach would certainly be an increase in disputes over CALEA implementation, and frequent repetition of rulemaking proceedings like the present one.

Instead of the "always been available" approach, Congress chose in Section 103(a) of CALEA to set out a specific list of assistance capability requirements, including that telecommunications carriers are required to provide only that call-identifying information that is "reasonably available" in their networks.[64] In many cases, Section 103(a) requires provision of substantially greater intercept assistance to law enforcement

[64] 47 U.S.C. § 1002(a)(2).

than has historically been available. On the other hand, in certain cases, the information provided to law enforcement under CALEA may be less than it has received in the past – or at least different.

Indeed, the information provided to law enforcement on wiretaps has always changed over time, and law enforcement has never been entitled to more information than is reasonably available to telecommunications carriers. Under Title III, the Supreme Court emphasized that "the power of federal courts to impose duties upon third parties is not without limits: unreasonable burdens may not be imposed."[65] This principle applies even where a carrier is being reimbursed for the cost of providing assistance, as required under Title III.[66] The principle has also been echoed by other courts and by Congress,[67] and remains the law today. DOJ and FBI do not cite a single case, nor apparently could they,

---

[65] United States v. New York Telephone Co., 434 U.S. 159, 172 (1977) (emphasis added).

[66] See 18 U.S.C. § 2518(4) ("Any . . . person furnishing . . . facilities or technical assistance shall be compensated therefore by [law enforcement] for reasonable expenses incurred in providing such facilities or assistance."). The district court in New York Telephone had required reimbursement of the costs of assisting law enforcement. See New York Telephone Co., 434 U.S. at 174.

[67] See In the Matter of the Application of the United States for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and a Terminating Trap, 610 F.2d 1148, 1155 (3rd Cir. 1979) (upholding order that "would cause a minimal disruption of normal operations," but stating that a challenge would be successful if a "greater burden" were shown); United States v. Mountain States Telephone and Telegraph Co., 616 F.2d 1122, 1132 (9th Cir. 1980) (upholding order that imposed "reasonable" obligations on telephone company, while acknowledging that "unreasonable burdens may not be imposed"). In each of these cases, as in New York Telephone, the government had been ordered to reimburse the company for the costs of assistance. See also S. Rep. No. 99-541, at 29 (1986) (telephone company customers "have a reasonable expectation, traditionally enhanced by telephone company practices and policies, that their company will not become, in effect, a branch of Government law enforcement") (report on ECPA).

in which a court has required a telecommunications carrier to provide, pursuant to a wiretap order, information that was not reasonably available to the carrier.

In addition, the DOJ/FBI Petition also lacks the factual detail regarding historical interception capabilities that would be needed to support the "always been available" argument – even if the argument were legally valid, which it is not. DOJ and FBI do not provide any factual support on interception practices from the particular cases, from other sources on wiretaps, or from affidavits of persons with experience in the area. In almost every case, the petition offers only anecdotal evidence regarding past practice on wiretaps. This deficiency is particularly significant because it is law enforcement that conducts wiretaps, and law enforcement that possesses almost all of the historical data on implementation of wiretaps. Court proceedings on issuance of wiretap orders rarely lead to published opinions that could provide historical evidence of wiretap practices.[68] Finally, with respect to several of the requests in the DOJ/FBI Petition, DOJ and FBI explicitly admit that the capabilities requested have not "always been available" on local loop interceptions – in fact, they admit some of the requested capabilities have not been available at all.

---

[68] DOJ and FBI have long been reluctant to provide public information about wiretap practice, or the legal authority for particular interception practices. In 1991, the DOJ issued a procedural handbook for prosecutors and investigators obtaining wiretap orders, see Department of Justice, Electronic Surveillance Manual, Volume I – Procedures and Forms, and stated that "Volume II of this manual, when issued, will discuss the applicable case law in the various areas of Title III, as well as both novel, and frequently arising, legal issues involved in Title III litigation," id. at Foreword. Volume II was never issued.

D. If the Commission Finds J-STD-025 "Deficient" in any Respect, It Should Return to TIA the Task of Amending the Standard

If the Commission does conclude that J-STD-025 is "deficient" in any respect, it should not adopt specific rules for CALEA compliance. Rather, it should indicate the areas of deficiency and return to TIA the task of setting industry standards. That is, while Section 107(b) of CALEA permits the Commission to establish CALEA compliance standards by rule, it does not require the Commission to do so.[69] Furthermore, the rules proposed in Appendix 1 to the DOJ/FBI Petition far overstate the requirements of CALEA and lack sufficient detail to permit telecommunications carriers and equipment manufacturers to determine the specific capabilities that must be implemented. The Commission should not reward DOJ and FBI for their continued approach of asking in general terms for maximum wiretap capabilities, without any tie to the specific requirements of CALEA.

The telecommunications industry drafted J-STD-025 and is best qualified to modify the standard pursuant to any instructions from the Commission. This approach of continued reliance on industry is strongly justified by the primary role of the telecommunications industry in standards-setting under CALEA, the technical complexity of the matters at issue, the lack of specificity in the DOJ/FBI Petition regarding the bases on which deficiency of J-STD-025 is asserted (which means the Commission lacks an adequate factual record to determine which capabilities should be mandated), and the fact

[69] See 47 U.S.C. § 1006(b).

that the industry is best positioned to adopt standards which provide for CALEA compliance while minimizing costs and impact on rate payers.

II. CALEA Does Not Require Delivery of Conference Call Conversations That Cannot Be Heard Over a Subscriber's Facilities

Only one of the capabilities requested in the DOJ/FBI Petition – i.e., the "ability to intercept the communications of all parties to a conference call supported by the subscriber's service or facilities"[70] – relates to the central purpose of CALEA of facilitating the interception of the content of communications. This fact demonstrates that J-STD-025 comprehensively provides for interception of call content and its delivery to law enforcement. Furthermore, the single additional capability requested by DOJ and FBI regarding conference calls is not required by CALEA, because the text of the statute explicitly limits required interception capabilities to communications "to or from" a subscriber, and because the DOJ/FBI request is based upon a significant and unwarranted expansion of the "facilities" doctrine.

The DOJ/FBI request is quite exceptional. It involves interception of conference call communications that do not involve any person directly using the telephone equipment or facilities at which an intercept order is directed. The request relates only to conversations between persons on hold who cannot be heard over the telephone of the intercept subject, and conversations between parties to the conference

[70] DOJ/FBI Petition at 27.

call after the intercept subject has hung up.[71] The CDT Petition addresses the requested capability in the following way:

> [T]he FBI would require carriers to build the capacity to monitor all parties to a multi-party call even after the subject of the intercept order is no longer participating in the call. The purpose of CALEA was to follow the target, not to facilitate monitoring of those left behind after the subject of the court order is no longer on the call.[72]

Furthermore, the DOJ/FBI Petition itself recognizes that the fact that this aspect of J-STD-025 "does not amount to a reduction in the information that has been available to law enforcement under POTS [Plain Old Telephone Service] . . . ."[73] In view of the insistence of DOJ and FBI that CALEA provides for no more than maintenance of historical interception capabilities, this admission is telling, and supports a conclusion J-STD-025 is not "deficient" for failure to require interception of conference call conversations that include neither the intercept subject nor anyone using the subject's facilities.

J-STD-025 provides for delivery of all communications that may be heard by any person using the intercept subject's facilities, including the communications of all participants in a conference call that may be heard over the facilities.[74] However, J-STD-

---

[71] See id. at 30 ("law enforcement would have no access to certain communications . . . in the event that the person using the subscriber's services placed some of the conferenced parties on hold or dropped off the call").

[72] CDT Petition at 12-13.

[73] DOJ/FBI Petition at 30.

[74] See J-STD-025 § 4.5.1 ("The Circuit IAP (CIAP) shall access a multi-party circuit-mode communication (e.g., Three-Way Calling, Conference Calling, or Meet Me Conferences) as it would be presented to the intercept subject.") (emphasis added)

025 does not provide for delivery of conference calls conversations involving no communications that are heard over the intercept subject's facilities, as requested by DOJ and FBI. While there may in certain circumstances be a legitimate law enforcement purpose for interception of some such communications,[75] this does not mean that there is a requirement under CALEA that telecommunications carriers deliver such communications to law enforcement. To the contrary, it is plain that no such requirement exists, either under CALEA or under the pre-existing law on Title III intercepts.

A. CALEA Only Requires Delivery of Conference Call Communications That Are "To or From" a Subscriber

CALEA requires interception only of communications "to or from equipment, facilities, or services of a subscriber . . . ."[76] By contrast, the conference call capabilities sought by the DOJ/FBI Petition involve communications that do not touch the subscriber's facilities at all or communications that merely transit a subscriber's facilities. The DOJ/FBI

---

[75] See DOJ/FBI Petition at 31-32. The DOJ/FBI Petition gives the example of a prisoner who calls a girlfriend (the intercept subject). The girlfriend then uses conference capability to include an associate of the prisoner, and hangs up, leaving the prisoner and associate on the line. See id. While the call between the prisoner and associate might provide evidence of criminal misconduct, it is not required to be delivered to law enforcement under CALEA for the reasons stated in this section. Furthermore, the information sought by the DOJ and FBI in this circumstance could easily be obtained by a Title III wiretap on the telephone used by the prisoner. See e.g. Crooker v. U.S. Dept. of Justice, 497 F. Supp. 500 (D. Conn. 1980) (interception by prison officials of personal telephone calls of prisoners did not violate Title III); United States v. Paul, 614 F.2d 115 (6th Cir. 1980) (same); United States v. Cheely, 814 F. Supp. 1447 (D. Alaska 1992) (same).

[76] 47 U.S.C. § 1002(a)(1) (emphasis added).

Petition glosses over these critical facts by using inexact language that fails to recognize relevant technical issues.

In many modern telephone systems, held or dropped segments of conference calls are entirely disconnected from the intercept subject's facilities. For example, in a Centrex system, a party on hold is disconnected by the central office switch from the circuit(s) supporting the conference call, and is connected to "quiet tone generator." Similarly, when a subscriber drops off a conference call, the circuit connecting the subscriber to the switch is dropped, and the conference call continues without any use of the subscriber's facilities. The communications sought by the FBI and DOJ in these circumstances plainly do not involve communications "to or from" a subscriber's facilities. Apparently recognizing this difficulty, the DOJ/FBI Petition seeks delivery of all conference call communications "supported by a subscriber's service."[77] While the intended meaning of this language in the DOJ/FBI Petition is not clear, it is clear that the language has no basis in the language of CALEA.[78]

---

[77] DOJ/FBI Petition at 32, 33.

[78] As noted above, the relevant provision of CALEA requires delivery of communications "to or from . . . services of a subscriber," 47 U.S.C. § 1002(a)(1) (emphasis added), not of communications "supported" by the subscriber's services. A held or dropped segment of a conference call is also not covered by CALEA where it involves communications that continue to transit a subscriber's facilities – i.e., where the communications cannot be heard over the subscriber's facilities, but electrical impulses of communications between persons at remote locations continue to pass through subscriber's facilities. While DOJ and FBI argue that the "to or from" provision of CALEA also covers such transiting portions of conference calls, DOJ/FBI Petition at 32, this argument ignores the consistent and critical distinction under Title III and other communications laws between originating/terminating traffic and transiting traffic. For example, for regulatory and ratemaking purposes, the Commission has long distinguished between traffic that originates or terminates in the United States and traffic that merely transits the United States on its way to a third country. See, e.g., Implementation and

(Continued ...)

B. The DOJ/FBI Request Is Inconsistent With the Law on Title III Interceptions

The DOJ/FBI request would also require an effectively unlimited, and unwarranted, expansion of the "facilities" doctrine of Title III. Because Title III provides the authority for wiretaps covered by CALEA, the lack of authority for an interception under Title III is critical to the Commission's analysis under CALEA. Put differently, if a wiretap capability would violate Title III, there cannot as a matter of law be an obligation to provide the capability under CALEA. Furthermore, the expansion of the facilities doctrine proposed by DOJ and FBI would violate the limits on wiretaps and other searches imposed by the Fourth Amendment of the Constitution.

Under the "facilities" doctrine, the authority of law enforcement to intercept communications carried over the facilities of the subscriber who is the subject of an intercept order, also allows interception of communications by persons other than intercept subject who use the facilities of the intercept subject.[79] However, the facilities doctrine is

---

Scope of the International Settlements Policy for Parallel International Communications Routes, 2 FCC Rcd. 1118, 1125 n.29 (1987) (certain reporting requirements apply to all traffic except transit traffic, which is defined as "traffic in which the U.S. carrier provides neither origination nor termination"); Establishment of Regulatory Policies Pursuant to the Communications Act of 1934 With Respect to Use of Communications Facilities in the United States by Foreign Entities for Communications Transiting the United States, Memorandum Opinion and Order, Mimeo No. 29209, Dkt. No. 19031 (rel. May 5, 1981) (Commission will not regulate transit traffic agreements). Similarly, Title III does not apply at all to traffic that transits the United States but is intercepted abroad. See, e.g., United States v. Cotroni, 527 F.2d 708, 711 (2d Cir. 1975) (Title III does not apply to foreign intercepts, even though intercepted communications traveled in part over U.S. facilities); Stowe v. Devoy, 588 F.2d 336, 341 n.12 (2d Cir. 1978) (same).

[79] See United States v. Kahn, 415 U.S. 143 (1974).

limited by the requirement that the intercept involve the actual telephone or other physical facilities of the intercept subject – as opposed to the entire system or network to which the telephones are attached. As one court has noted, "'facilities' means the target telephones."[80] Furthermore, the DOJ/FBI Petition acknowledges that the "facilities" have historically been considered for Title III purposes as the subscriber's "terminal equipment,"[81] and that "interception orders under Title III are directed at particular telecommunications facilities."[82]

Despite these clear limitations on the facilities doctrine, DOJ and FBI contend that Title III "focuses on the subscriber's facilities and services,"[83] and that "[i]n practice, the facility is described by the subscriber's telephone number, which would entail network facilities that support and are identifiable with the service associated with that telephone number."[84] In other words, in law enforcement's view, any equipment in a carrier network that is used to provide a service to a particular telephone number becomes the "facility" of the subscriber. This argument would effect a huge expansion of the facilities doctrine, and

---

[80] United States v. Tavarez, 40 F.3d 1136, 1139 (10th Cir. 1994); see also 1 James G. Carr, The Law of Electronic Surveillance § 4.4(c)(2) (2d ed. 1998 Supp.).

[81] See DOJ/FBI Petition at 30 (stating that it would "not amount to a reduction in the information that has been available to law enforcement" to interpret CALEA as limiting law enforcement to the ability to intercept "[a]s long as the subscriber's terminal equipment is connected").

[82] DOJ/FBI Petition at 28.

[83] DOJ/FBI Petition, at 32 (emphasis added); see also id. at 30 ("Title III interception orders authorize law enforcement to acquire all criminal communications of all parties conversing over the subscriber's facilities or services . . .").

[84] DOJ/FBI Petition at 28 n.10.

intentionally blurs the critical distinction in Title III between the subscriber's facility and the subscriber's service.[85] Title III draws a "bright line" around the subscriber's facilities, and does not require carriers to deliver communications over facilities not associated with the subscriber.

This limitation of the "facilities" doctrine to the particular telephone equipment of the subscriber is also required by the particularity requirement of the Fourth Amendment to the Constitution.[86] Congress' recognized this requirement when it enacted Title III.[87] Eliminating the required link to the subscriber's facilities (or to the specific facilities identified) would take the interception far afield from the particular persons and places with regard to which law enforcement has established probable cause. In the situation where an intercept subject is no longer participating in the conference call, law enforcement would be listening to conversations in which neither the requisite person nor the requisite

---

[85] See 18 U.S.C. § 2518(4) (requiring access only to "information, facilities, and technical assistance").

[86] See Kahn, 415 U.S. at 157 (wire interception order may be issued when "there is probable cause that a particular telephone is being used to commit an offense"). When the call does not involve any facilities identifiable with the subscriber, interception does not involve the "particular" facilities required by the Fourth Amendment. See also United States v. Donovan, 429 U.S. 413, 427 n.15 (1977) ("In the wiretap context, [the Fourth Amendment] requirements are satisfied by identification of the telephone line to be tapped and the particular conversations to be seized.").

[87] See S. Rep.1097 at 102 (1968) (Section 2518 "requires a finding of probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense . . . . With the findings required by subparagraphs (a) and (b) [of Section 2518], the order will link up specific person, specific offense, and specific place. Together they are intended to meet the test of the Constitution that electronic surveillance techniques be used only under the most precise and discriminate circumstances, which fully comply with the requirement of particularity.").

facilities are present. Essentially, law enforcement simply would be listening for any criminal activity, without any prior showing of probable cause as to the persons or facilities involved. This approach is particularly troublesome in view of the fact that even where probable cause has been found to exist for an intercept, approximately 80 percent of intercepted conversations are non-incriminating.[88]

The DOJ/FBI argument also fails because Section 2518 only authorizes law enforcement access to communications that can be heard over the targeted facilities, not access to communications that are merely connected through the targeted facilities. The DOJ and FBI argue that under United States v. Kahn the government may "intercept any communications carried over the facilities covered by the order and are otherwise within the scope of the order, even if the individual under investigation does not participate in such communications."[89] Yet the Kahn decision is limited to communications "to and from the two named telephones concerning criminal activities," which the Court viewed as a subset of "communications of anyone who talked on the named telephone line."[90] Kahn

---

[88] See Administrative Office of the United States Courts, Annual Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications -- 1997, Table 7 (April 1998) (reporting an average of 2,081 intercepted communications and an average of 418 incriminating intercepted communications per installed wiretap).

[89] DOJ/FBI Petition at 29 (emphasis added) (citing Kahn).

[90] Kahn, 415 U.S. at 147, 154.

did not authorize access to communications that cannot be overheard on the named telephones, but are merely connected through or "carried over" the facilities involved.[91]

III. CALEA Requires Delivery of Call-Identifying Information That Is "Reasonably Available" to Telecommunications Carriers

The DOJ/FBI Petition includes a variety of requests for capabilities purporting to relate to "call-identifying information" covered by CALEA. The Commission should reject these requests for several reasons, including the fact that they are based upon incorrect application of two critical and relevant provisions of CALEA.

First, CALEA defines "call-identifying information" as:

> dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.[92]

J-STD-025 contains a further definition of "call-identifying information," which DOJ and FBI do not allege to be deficient:

> As interpreted by this Interim Standard: **destination** is the number of the party to which a call is being made (e.g., the called party); **direction** is the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g., redirected-to party or re-directed from party); **origin** is the number of the party initiating a call (e.g., calling

---

[91] See also United States v. Shipp, 578 F. Supp. 980, 987 n.18 (requirements of the Fourth Amendment were met by limiting the wiretap order to conversations over telephone line that involved the enumerated offenses).

[92] 47 U.S.C. § 1001(2) (emphasis added).

party); and **termination** is the number of the party ultimately receiving a call (e.g., answering party).[93]

As detailed below, several of the capabilities that DOJ and FBI request as call-identifying information do not fall within the scope of these definitions.

Second, the DOJ/FBI Petition entirely ignores the basic CALEA standard for delivery of call-identifying information – i.e., that telecommunications carriers must deliver only "call-identifying information that is reasonably available to the carrier . . . ."[94] The legislative history of CALEA specifically provides that "if [call-identifying] information is not reasonably available, the carrier does not have to modify its system to make it available."[95] Thus, where telecommunications equipment and networks designed to satisfy customer needs do not generate a particular type of call-identifying information – i.e., where there is no business purpose for making such information available – CALEA plainly does not require that the information be delivered to law enforcement.

The DOJ/FBI Petition entirely ignores the explicit "reasonably available" limitation in CALEA, and instead advances a variety of other non-statutory bases for provision of the requested capabilities. In some places, the DOJ/FBI Petition appears to take a view that carriers must deliver all call-identifying information that law enforcement believes is useful. In other places, the DOJ/FBI Petition seeks delivery of any call-identifying information that bears even a passing resemblance to information acquired on

---

[93] J-STD-025 at 5 (definition of "call-identifying information") (original emphasis).

[94] 47 U.S.C. § 1002(a)(2) (emphasis added).

[95] CALEA House Report at 22 (emphasis added).

interceptions at some unspecified time in the past, even where the evidence regarding such prior interceptions is no more than anecdotal and even where the interception technology used in the past is radically different from modern technologies. Regardless of whether these justifications proffered by DOJ and FBI have merit as a matter of law enforcement policy, it is plain that they are not supported by CALEA. Rather, the statutory standard for whether call-identifying information must be provided under CALEA is whether it is "reasonably available."

The remainder of this section considers these major flaws of the DOJ/FBI Petition, as well as various other defects, with respect to each requested capability related to call-identifying information. The clear conclusion for the Commission with respect to each such capability should be that the existing provisions of J-STD-025 are not "deficient."

A. Subject-Initiated Dialing and Signaling

Two of the capabilities requested in the DOJ/FBI Petition – "post-cut-through dialing" and "subject-initiated signaling activity" – involve information generated by actions taken by the intercept subject. These capabilities are addressed together as "subject-initiated dialing and signaling activity" in DOJ/FBI Petition.[96]

[96] See DOJ/FBI Petition at 36-42.

1. Post-Cut-Through Dialing

The DOJ/FBI Petition includes "post-cut-through dialing information" in its discussion of subject-initiated dialing and signaling. While these issues are related, post-cut-through dialing requires separate analysis, as DOJ and FBI recognized by including it as a separate item in the "punch list."[97] Significantly, J-STD-025 already requires delivery of post-cut-through dialing information to law enforcement.

Post-cut-through dialing information consists of numbers dialed after a call circuit has been completed by the carrier to which an intercept order is directed. That is, a call is "cut through" when a circuit to the called party has been completed.[98] Subscribers may dial post-cut-through digits for a variety of purposes, most of which are without question not call-identifying information under CALEA – for example, responses to a automatic queuing system (i.e., a system that says things like "please dial 4 if you want to learn more about travel to Hawaii"), entry of a credit card to pay for a call or for other purposes, or entry of information that will be transmitted to a pager. However, where the initial call is completed to another telecommunications carrier, post-cut-through digits may relate to the further routing of a subscriber's call – for example, when the subscriber dials an 800 number to connect to a long distance company, and then dials further digits to complete the call.[99] While J-STD-025 does not treat such post-cut-through digits as call-

---

[97] See Colgate Letter at 2 & Attachment A.

[98] There is no need to address pre-cut-through dialing, because there is no dispute over the requirement of J-STD-025 that pre-cut-through dialed digits be provided on the call data channel. See J-STD-025 § 5.4.5 (describing Origination message).

[99] See DOJ/FBI Petition at 41.